



(877) 2 FAX LEO
(877) 232-9536
402 Johnston Hall
Baton Rouge, LA 70803

Page 1

Law Enforcement Online LEO International User Application

WARNING

LEO is an official U.S. Government system for authorized use only by authorized members of the law enforcement, criminal justice and public safety community. Information presented in this system is considered sensitive but not classified and is for official law enforcement/criminal justice/public safety use only. The use of this system will be monitored for security and administration purposes and accessing this system constitutes consent to such monitoring. Any unauthorized access of this system or unauthorized use of the information provided on the LEO network is prohibited and may be subject to criminal and civil penalties under federal law.

This FBI system is for the sole use of authorized users for official business only. You have no expectation of privacy in its use. To protect the system from unauthorized use and to insure that the system is functioning properly, individuals using this computer are subject to having all their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals evidence of possible abuse or criminal activity, system personnel may provide the results of such monitoring to appropriate officials.

LEO will collect and store system and network related information in a persistent cookie. The purpose of collecting and storing this information is so that LEO can enhance its security by employing advanced authentication reliant on this information. The information is encrypted and LEO will not share this with any unauthorized parties.

Warning! The use of publicly accessible computers (e.g. libraries, airports, cafes, hotels, etc.) to access LEO is unauthorized. This type of usage may result in the involuntary dissemination of information to unauthorized entities. Data may be left on this computer resulting in the next person using this machine the ability to view your data.

PRIVACY ACT STATEMENT

General - This information is provided pursuant to Public Law 93-579 (Privacy Act of 1974) for individuals completing LEO user application forms. Authority - LEO is a federally funded national communications system established by the FBI. Application information is solicited under the authority of the Federal Records Act (Title 44, United States Code) and implementing regulations (Title 36, Code of Federal Regulations, chapter XII). Purpose and Use - The principal purposes of LEO user application forms are to collect information needed to determine qualifying factors for authorized use, and verification of identity. This completed application will be used to register this account as a qualified LEO account. All or part of the submitted information may be disclosed outside the FBI to federal, state, local, or tribal law enforcement agencies charged with the responsibility of investigating a violation or potential violation of the law and to applicant agency or organization to periodically verify continued access to LEO. Disclosure may otherwise be made pursuant to the routine uses most recently published in the Federal Register for the FBI's Central Records System (Justice/FBI 002). Failure to provide the requested information shall result in the denial of this application.

Instructions: Type or write in the information requested. When completed, fax or mail to the information provided in the upper right hand portion of page one of this form. Send all pages. If you require additional space to include information, please attach extra sheets and reference the appropriate section. **IMPORTANT:** Non-legible applications will not be processed.

1. Applicant Information

Applicant Name (Surname/Family Name, First, MI) :	
Title / Position:	
Email Address:	
Employing Agency and/or Organization:	
Address:	Country of Birth:
	Country of Residence:
Phone:	Country of Citizenship:
Fax:	State/Province/County:
	City: Postal Code:
Are you a US Citizen? Yes No Dual	
Please list all citizenships held other than US:	

2. Security Verification Information

Passport #/Country &/or last 6 of SSN if US Citizen:	Date of Birth:
Code Word (ex: mother's maiden name):	Gender: Male Female
Are you a Law Enforcement Officer? Yes No If other please specify:	

3. Applicant Certification

I hereby certify that I am an employee of the duly constituted law enforcement/criminal justice/public safety agency described above in this application and that I understand and consent to the terms of this application, including the provisions set out in the Warning and the Privacy Act Statement, and agree to abide by all such provisions.

X

APPLICANT SIGNATURE

MONTH / DAY / YEAR



LEO International User Application Page 2

Instructions Sections 4,5,6: These areas are reserved for the LEGAT, ALAT, or Other FBI Designated Authority responsible for the requested account. Complete all requested information where applicable.

4. LEGAT / ALAT / Other FBI Designated Authority (Responsible Party)

Name (Last, First, MI):

Legat/Division/Field Office:

Title / Position:

Email Address:

Room Number:

Address:

Country:

Zip:

State / Prov:

Phone:

City:

Fax:

5. Justification of Access, Name & Description of Project

Justification For Access:

Is this a Special Project? Yes No

Describe Special Project (if applicable):

Length of Access (if applicable)

From: MONTH / DAY / YEAR

To: MONTH / DAY / YEAR

Type of Access (Select One):

LEO Email Only

LEO Email & Specific SIG

Specify SIG:

6. LEGAT / ALAT / Other FBI Designated Authority Certification (Please complete signature lines)

I hereby certify that the above named individual is an employee of the duly constituted agency and/or organization described above and is authorized to have access to the Law Enforcement Online (LEO) system.

X

SIGNATURE

MONTH / DAY / YEAR

Please Print Name:



**Instructions for LEGAT / ALAT /
Other FBI Designated Authority
Administration:**

Fax: (877) 232-9536

LEO Administration Only

SIG **VPN**

X

MONTH / DAY / YEAR

X

MONTH / DAY / YEAR

[illegible]

**FD-889**

Revised 09/18/07
Previous Versions
Obsolete

**FBI Information Technology and Information Systems
Rules of Behavior for General Users Agreement Form**

Purpose: This agreement outlines the acceptable and unacceptable uses of FBI Information Technology (IT) and Information Systems (IS). It also outlines the signer's responsibilities regarding stewardship and use of FBI IT/IS and Public Key Infrastructure (PKI) assets and capabilities if a PKI token is issued.

Scope: This agreement applies to anyone granted access to any FBI IT/IS, including but not limited to: FBI employees, contractors, interns, detailees, and personnel from Other Government Agencies (e.g., Federal, state, municipal, or tribal). All references to IT/IS monitoring herein pertain to data communications only (emails, facsimile, computer database use and data storage, digital transmission of data...etc.) and does not apply to voice communications. This agreement form must be signed before access to any FBI IT/IS is granted.

References:

- Standards of Ethical Conduct Regulation (5 CFR Parts 2635 and 3801).
- The Federal Information Security Management Act (FISMA) of 2002.
- The FBI Security Policy Manual (SPM).
- FBI Manual of Investigative Operations and Guidelines (MIOG) Part II Section 16-18, and 26.
- FBI Manual of Administrative Operations and Procedures (MAOP) Part II Section 2-1.1.
- FBI Unclassified Network (UNet) Policy Version 1.0, 3 April, 2007
- U.S. Department of Justice (DOJ) Public Key Infrastructure X.509 Certificate Policy v1.13, 15 December, 2006.
- X.509 Certification Practices Statement for the Federal Bureau of Investigation High Assurance Certificate Authority v3.0, 31 October 2005.
- FD-1001 (1-22-2007) DOJ Consent For Warrantless Searches Of Department Of Justice Workplaces.

Statement of Responsibility: I am responsible for all IT that I introduce into FBI space including devices that are privately owned, or those owned by another government agency. I am responsible for all activity on FBI IS's, as well as any other IT/IS's that are authorized to operate in FBI space, that occurs on my individual account(s) once my logon credential or password has been used to logon. If I am a member of a "group account," I am responsible for all activity when I am logged on an IS associated with that account. I acknowledge that the ultimate responsibility for ensuring the protection of FBI non-public information lies with me, the user of FBI IS's and non-FBI IT/IS's authorized to operate in FBI spaces.

Access: Access to FBI IT, IS, networks, and other agency systems operating in FBI spaces is for official and authorized purposes as set forth in Title 5 CFR Parts 2635 and 3801 (Federal Ethics Regulations) (noted above) and as further outlined in this document.

Revocability: The ability to use IT in FBI space and access to FBI IS's is a revocable privilege. IT used in FBI space is subject to vulnerability assessment, content monitoring and security testing.

Rules of Behavior: I will adhere to the following Rules of Behavior (ROB):

1. I consent to monitoring or search of any IT/IS equipment or media I bring into, or remove from FBI owned, controlled or leased facilities. When asked by authorized personnel I will provide unfettered access to all equipment or media brought into or removed from such FBI facilities. I also understand that FBI or FBI leased IS's may be monitored or otherwise accessed for law enforcement or other compliance purposes and my agreement to this FBI ROB constitutes my consent to be monitored and to allow access to FBI IS's accessed by me.

**FD-889**

Revised 09/18/07
Previous Versions
Obsolete

**FBI Information Technology and Information Systems
Rules of Behavior for General Users Agreement Form**

2. The following (2.a.) applies **only** to personnel from Other Government Agencies whose duties require them to bring IT/IS assets (e.g., laptop or desktop computers) owned or leased by their parent agency into FBI facilities:
 - a. I understand that the aforementioned IT/IS assets are also subject to FBI search and/or monitoring; however, prior to any search or monitoring the FBI will coordinate with the appropriate Security Personnel or other responsible representatives of my parent agency to afford my agency an opportunity to provide warnings to the FBI about the types of information that may exist within my IT/IS devices and to ensure that my agency is afforded the opportunity to have appropriate representation during any and all searches.
3. I will comply with the FBI SPM, MAOP, MIOG and local Standard Operating Procedures and I will address any questions regarding policy, responsibilities, and duties to my Information System Security Officer (ISSO), Information System Security Manager (ISSM), or Chief Security Officer (CSO).
4. I will protect my password(s) in accordance with the classification level of the system or at the highest classification of the data being secured.
5. I will only use strong passwords as defined in the FBI SPM and agree to change my password with a frequency as specified by policy or as requested for security reasons.
6. I will use screen locks or logoff my workstation upon departing the immediate area.
7. I will use all required virus-checking procedures before accessing information from all removable media or before accessing email attachments from unknown sources.
8. I will mark all media (fixed and removable) with the appropriate classification level and ensure that it is properly safeguarded.
9. I will NOT disseminate any FBI non-public information to anyone who does not have a verified authorization to access the information and appropriate security clearance.
10. I will complete the FBI's Annual INFOSEC Awareness Training or provide my ISSO, ISSM or CSO with adequate documentation of my completion of my employing agency's annual information security training.
11. If designated as a "*Privileged User*" I will complete the required Privileged User Security training and sign the *Privileged User* Rules of Behavior form.
12. I will immediately report any suspicious incidents or improper use to my ISSO, ISSM, or CSO in accordance with SPM guidelines.
13. If issued digital certificates by the FBI PKI Certification Authority (CA), in addition to the above I will:
 - a. Use the certificate and corresponding keys exclusively for authorized and legal purposes for which they are issued and only use key pairs bound to valid certificates. Note: Explanation of what certificates, keys, and key pairs are and how to use them is explained on the PKI Registration Form when the token is issued.
 - b. Re-authenticate my identity to the FBI CA in-person and register for certificate re-key at least once every three years, or as instructed by designated authorities.
 - c. Protect my token and private keys from unauthorized access and be aware of the location of my token and ensure its security at all times, whether in my immediate possession, in FBI space, or in my home.
 - d. Use the "strong password" guidance mentioned in 4 and 5 above.
 - e. Immediately request my ISSO, ISSM, or CSO or an authorized FBI PKI authority to revoke my associated credentials if I suspect that my token or keys are lost/stolen or if my password was compromised.

**FD-889**

Revised 09/18/07
Previous Versions
Obsolete

**FBI Information Technology and Information Systems
Rules of Behavior for General Users Agreement Form**

Expressly Prohibited Behavior: I will **NOT** conduct or participate in any of the following behaviors or activities on any FBI IT, IS, or on other agency IT/IS systems authorize to operate in FBI space, unless required as part of my official duties:

1. Reveal my password to anyone or permit anyone to use my account, user ID, or password(s).
2. Tamper (e.g., alter, change, configure, install software or hardware, or connect IT or systems) with my computer to circumvent any FBI policy and IT/IS protections.
3. Install or connect non-FBI owned or leased (including privately owned) software or hardware (e.g., PEDS, such as Palm Pilots, Blackberrys, MP3 Players...etc.) and removable media (e.g., thumb drives, memory sticks...etc.) to FBI IT/IS.
4. Connect classified IT or IS's to the Internet or other unclassified systems.
5. Introduce wireless devices into FBI space without authorization from the ISSM.
6. Download, view, or send pornography or obscene material.
7. Download, view, or send matter that involves racist, discriminatory, supremacist or "hate" type causes.
8. Access, retrieve, create, communicate or print text or graphics that are generally inappropriate or unprofessional.
9. Engage in email hoaxes, gossip, chain emails, forwarding virus warnings, or advertisements (spam).
10. Use FBI IT/IS or FBI non-public information for personal benefit, profit, to benefit other persons, non-profit business dealings, any political (e.g., lobbying or campaigning) party candidate or issue or for any illegal activity.
11. Knowingly violate any statute, such as copyright laws or laws governing disclosure of information.
12. Attempt to process or enter information onto a system exceeding the authorized classification level. (e.g., placing Top Secret information on Secret Enclave).
13. Use internet "chat" services (e.g., AOL, Instant Messenger, Microsoft Network IM, Yahoo IM...etc).
14. Download Peer-to-Peer file sharing software or applets, or to use any other means to download music, video or game files.
15. Introduce executable code (such as, but not limited to, .exe, .com, .vbs, or .bat files).
16. Create or intentionally spread malicious code (i.e. viruses and Trojans).
17. Attempt to circumvent access controls/permissions or hack into (e.g., by penetration testing, password cracking, "sniffer" programs, etc.) any FBI IT/IS.
18. Attempt to circumvent access controls or to use unauthorized means to gain access to accounts, files, folders or data on FBI IT/IS.
19. Use an account, User ID, or password not specifically assigned to me, masquerade as another user, or otherwise misrepresent my identity and privileges to IT/IS administrators and security personnel.
20. Setup automatic forwarding of email to non-government accounts (e.g., Gmail, Yahoo, Hotmail, business/vendor email accounts, etc.).
21. Download attachments via Outlook Web Access to a non-government computer.
22. Remove sensitive/classified media (paper or electronic) from controlled areas/facilities (i.e. taking classified media home) without authorization.

Privacy Act Statement:

The information solicited on this form is collected pursuant to the Federal Information Security Management Act (FISMA) of 2002, the Computer Security Act of 1987, the general recordkeeping provision of the Administrative Procedures Act (5 U.S.C. § 301) and Exec Order 9397, which permits the collection of social security numbers. The Public Key Infrastructure (PKI) portion of this agreement is collected pursuant to 5 U.S.C. §§ 3301, 9101, Exec. Order No. 12,968, Exec..



FD-889

Revised 09/18/07
Previous Versions
Obsolete

FBI Information Technology and Information Systems Rules of Behavior for General Users Agreement Form

Order No. 10,450, and 28 C.F.R. § 0.138. Pursuant to the Privacy Act of 1974, 5 U.S.C. § 552a, we are providing the following information on principal purposes and routine uses. The principal purpose of this form is to verify that individual signatories are aware of the rules of behavior that govern access to FBI IT/IS that operate in FBI space. If a digital certificate from the FBI PKI is issued, this form also supports the operation of the PKI Program, which is designed to increase the security posture of the FBI. For the PKI Program, the information submitted will be used to verify user identity in support of the digital signatures and data encryption/decryption provided by the FBI PKI system. This information, in conjunction with the PKI digital signatures and data encryption/decryption, is used to provide Authentication, Non-repudiation, and Confidentiality services.

The information on this form may be shared within the Department of Justice (DOJ) components and with other governmental agencies for the purpose of providing access to these facilities, facilitating information sharing (i.e.-sending encrypted e-mails), and for other authorized purposes. In addition, information may be disclosed to the following:

1. Appropriate federal, state, local, tribal, foreign or other public authorities conducting criminal, intelligence, or security background investigations.
2. Officials or employees of other federal agencies to assist in the performance of their duties when disclosure is compatible with the purposes for which the information was collected.
3. To contractors, grantees, experts, consultants, or others when necessary to accomplish an agency function.
4. Pursuant to applicable routine uses for the FBI's Central Records System (Justice/FBI-002), which is where the information solicited on this form will be maintained.

The provision of the information is voluntary, but without your acknowledgment of the rules of behavior for accessing FBI information, and IT/IS's that operate in FBI space, you may not be permitted such access or receive FBI PKI credentials and certificates, which may affect your ability to perform your official duties. Disclosure of the last four digits of your social security number is also voluntary, but will help to differentiate you from other individuals with the same or a similar name.

Acknowledgment

I acknowledge that I have read and understand the above listed Rules of Behavior. I also state that I will adhere to these Rules of Behavior and that failure to do so may constitute a security violation resulting in denial of access to FBI IT/IS networks or facilities. I also understand that violation of these Rules of Behavior will be reported to the appropriate authorities for further administrative, civil or criminal disciplinary action deemed appropriate.

Printed Name: _____ Date: _____

Employee Signature: _____ Last Four of SSN: xxx-xx-____ _

FBI Personnel File Number (if known): _____

Note: If applicable, other Govt. Agency (Federal, state, or municipality) _____

Filing Instructions: Completion of the FBI's annual INFOSEC Awareness Training satisfied the signatory and acknowledgement requirements for the purpose of storage and audit of this form. When a hardcopy is required, CSOs are responsible for filing this form IAW EC 319W-HQ-A1487698-SECD Serial 63 Form Owner: Career Services Management Unit, FBI SecD